☰

The dark side of the coin: Bitcoin and crime

Published on: Sep 5, 2017 | by Zoe Gross

Bitcoin has been riding an impressive wave, recently reaching an all-time high of over US$4600, and more than tripling in value for the year. It's now nearly three times the price of gold.

But with cryptocurrency's potential to radically transform entire monetary systems, also comes a darker side (and we're not talking about Whoppercoin).

Bitcoin's underlying blockchain technology offers would-be cyber criminals two distinct advantages. By operating as a decentralised currency, whereby people pay each other without a middle man (like a bank or other financial institution), it provides a considerable amount of anonymity.

Bitcoins can be held in virtual wallets identified only by a number. According to a recent Cambridge University study, as many as six million people around the world have a wallet of this kind, and spend bitcoins on goods from the increasing number of retailers now accepting the currency, as well as illicit goods like drugs and firearms on the digital black market.

Sometimes perceived as the "wild west of finance", the cryptocurrency space has been connected to various scams, hacks and other criminal activities which have taken advantage of this anonymity.

A very brief history of crypto crime

currency, Silk Road was a black market trading site buried deep in the 'darkweb', a corner of the internet not indexed by search engines or accessible to those without authorisation.

In March of the same year, Tomáš Jiříkovský was arrested in the Czech Republic for allegedly stealing millions of dollars in bitcoin from Sheep Marketplace, one of the 'darknet' markets that gained popularity after the fall of Silk Road 1.0.

Then, in September 2015, 33-year-old American Trendon Shavers pleaded guilty to running a $150 million Ponzi scheme, the first Bitcoin securities fraud case.

Also in 2015, 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of $390 million from the now shuttered Tokyo-based bitcoin currency exchange, Mt. Gox.

More recently, beginning around May this year, the now infamous ransomware attack, WannaCry, locked files on corporate and government computers worldwide and demanded payment into certain bitcoin addresses in exchange for unfreezing those files. The transactions can be monitored online in real time. Victims have paid more than $101,000 in bitcoin to the attackers.

The end of Bitcoin?

Well, no.

Certainly, situations like these have given rise to multiple calls for a global Bitcoin ban. But not only would this be a kind of baby with the bathwater response, it also would not be that easy.

According to Richard Henderson, global security strategist at data security firm, Absolute: "Getting rid of Bitcoin to stop ransomware would be like the US Government getting rid of $100 bills to try to stop drug dealers from laundering their dirty money."

This, Henderson told *CEO Magazine*, is not the right solution. "Would it momentarily create a bump in the road for cyber attackers who are making millions off ransomware?" he posits. "Absolutely, but only for a fleeting moment."

Moreover, as John Bohannon writes in *Science*, "The majority of Bitcoin users are law-abiding people motivated by privacy concerns or just curiosity."

Jerry Brito is executive director of Coin Center, a Bitcoin research and advocacy group, as well as one of the founding companies behind Blockchain Alliance, a resource for law enforcement and regulators.

Brito writes in a blog post: "Law enforcement will pursue criminals no matter what technology they're using, and how law enforcement does this can affect an open technology."

"As a result, it's in everyone's interest — law enforcement, industry, and those of us who want to keep the technology free and open — to make sure that law enforcement understands how the technology works, what can and can't be done with it, and what are the opportunities and limits it presents for their investigations."

Regulation as best practice – Japan leads the way

This more knowledge-based approach also hinges on the importance of a sound regulatory framework. Mt. Gox's bankruptcy prompted Japan's government to make decisions around how to treat Bitcoin, and preceded a push by local regulators to license cryptocurrency exchanges.

In this light, Japan became the first country to regulate cryptocurrency exchanges at the national level in April this year, part of a government effort to harness financial technology as a means of stimulating the economy.

Japan's regulations help prevent misuse of Bitcoins and other cryptocurrencies for illegal activity, and include requiring banks and other businesses to verify identities, keep records and report suspicious transactions.

The European Union has also been discussing how to impose rules on Bitcoin exchanges as part of its Fourth Anti-Money Laundering Directive.

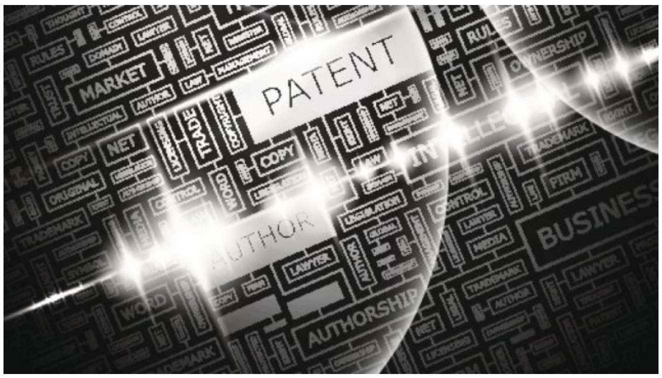
In line with these kinds of efforts to prevent money laundering, Australia recently introduced a bill that regulates Bitcoin exchanges.

Such regulatory frameworks rethink the way we define commodities themselves. Japan, for example, now considers anything that can be exchanged for goods and services or legal tender as a currency, including not just Bitcoin, but a whole range of cryptocurrencies – even Dogecoin.

If you like this, you may like ...

58 insane facts about Bitcoin

An overview of digital currencies



Astute management of intellectual property never more critical

DigitalX about to go live with AirPocket

☰

Accordingly you should consider how appropriate the advice (if any) is to those objectives, financial situation and needs, before acting on the advice.

Conflict of Interest Notice

S3 Consortium Pty Ltd does and seeks to do business with companies featured in its articles. As a result, investors should be aware that the Firm may have a conflict of interest that could affect the objectivity of this article. Investors should consider this article as only a single factor in making any investment decision. The publishers of this article also wish to disclose that they may hold this stock in their portfolios and that any decision to purchase this stock should be done so after the purchaser has made their own inquires as to the validity of any information in this article.

Publishers Notice

The information contained in this article is current at the finalised date. The information contained in this article is based on sources reasonably considered to be reliable by S3 Consortium Pty Ltd, and available in the public domain. No "insider information" is ever sourced, disclosed or used by S3 Consortium.

Q & A

Trek Metals Aim To Live Long and Prosper

Abundant Produce takes a purely organic approach to skin care

How SWF is disrupting the finance industry

Q&A with Anthony Hall, Executive Director at American Pacific

Most Popular

Vector reveals JORC upgrade for Adidi-Kanga Gold Project

AUZ pens pivotal cobalt-nickel offtake deal

Artificial Intelligence – human friend or foe?

Castillo drills significant massive sulphide mineralisation at Cangai Copper Mine

Today's Top Stories

Northern Minerals poised to capitalise on Trump's resources policy

MGC Pharma releases operational and strategy update

Roots releases exceptional pilot results

EHR Resources commences next stage of exploration at La Victoria

Editor's Pick

CPH on track to tap multi-billion-dollar Canadian cannabis market

Global companies line up to trial FGO's ROSIE AI

5 economic questions Australia faces in 2018

Turning a new leaf: 5 medical cannabis trends for 2018

Connect with us

Customer Notice | Privacy Policy | Financial Services Guide | Disclosure Policy | Contact